UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

GARY NICKERSON, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. WAWA, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

INTRODUCTION

1. This class action seeks redress for negligence because of the failure of Wawa, Inc. ("Wawa") to implement and maintain reasonable security measures to protect consumers' personally identifiable information.

JURISDICTION AND VENUE

2. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

3. This Court has jurisdiction over Wawa because it is a Pennsylvania company with its principal headquarters here, it regularly conducts business in Pennsylvania, has sufficient minimum contacts in Pennsylvania and has intentionally availed itself of this jurisdiction by marketing and selling products in Pennsylvania and other consumers nationwide."

4. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District.

PARTIES

5. Plaintiff Gary Nickerson is a citizen of the State of Pennsylvania who resides in Bucks County.

6. Defendant Wawa, Inc. is a New Jersey corporation with its principal place of business located at 260 West Baltimore Pike, Wawa, Pennsylvania 19063.

FACTS

7. Wawa is a chain of more than 850 convenience stores located across the east coast of the United States, operating stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Among other products, Wawa convenience stores offer built-to-order foods, beverages, coffee, as well as fuel services.

8. In the course of providing its services to consumers, Wawa accepts payments by debit card and credit card.

9. Plaintiff and his wife regularly purchase gasoline, coffee, and other items from Wawa convenience stores, often using Plaintiff's credit card account, for which Plaintiff's wife is also an authorized cardholder.

10. Plaintiff's wife purchased coffee and gasoline a few times a month from the Wawa convenience store located at 3901 Aramigo Avenue, Philadelphia, Pennsylvania 19137 through December 19, 2019.

11. Plaintiff and his wife have also recently purchased goods at the following Wawa convenience store locations:

i. 656 Old Bridge Turnpike, South River, NJ 08882;

ii. 1528 Trenton Road, Langhorne, Pennsylvania 19407; and

iii. 132 Oxford Valley Road, Langhorne, Pennsylvania 19056.

12. On or about December 19, 2019, Wawa issued a Press Release entitled *Wawa Data Security – Updates & Customer Resources*, which announced that "Wawa has experienced a data security incident." (hereinafter, the "Data Breach").

13. This press release stated, in part:

> Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. At this time, we believe this malware no longer poses a risk to Wawa customers using payment cards at Wawa, and this malware never posed a risk to our ATM cash machines.
>
> …
>
> **What Happened?**
>
> Based on our investigation to date, we understand that at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware. We also immediately initiated an investigation, notified law enforcement and payment card companies, and engaged a leading external forensics firm to support our response efforts. Because of the immediate steps we took after discovering this malware, we believe that as of December 12, 2019, this malware no longer poses a risk to customers using payment cards at Wawa.
>
> **What Information Was Involved?**
>
> Based on our investigation to date, this malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on

December 12, 2019. Most locations were affected as of April 22, 2019, however, some locations may not have been affected at all.[1]

14. The Data Breach was reportedly the result of malware installed on Wawa's payment process servers.

15. According to Wawa's press release, the Data Breach affected customers who made card purchases either in store or at a fuel pump.

16. As a result of the Data Breach, the personal credit card information (hereinafter, the "Personal Information") of customers who made such card purchases at Wawa convenience stores and fuel pumps were exposed to malicious actors, including customer's names, credit card numbers, and expiration dates.

17. According Wawa's press release, the Data Breach began as early as March of 2019 and may have affected all Wawa locations as early as April 22, 2019.

18. Due to Wawa's failure to detect the Data Breach, malicious actors were able to exfiltrate customer's Personal Information through December of 2019, a period of roughly nine months.

19. Although Wawa claims the Data Breach "no longer poses a risk to Wawa customers using payment cards at Wawa," Wawa appears to be unaware of the parties who were responsible for the breach as well as the method by which such parties compromised Wawa's security systems.[2]

Wawa Failed to Abide by Industry Standards for Protection of Customer Card Information

[1] *See* https://www.wawa.com/alerts/data-security (last accessed Dec. 26, 2019).

[2] *See* Christian Hitch, *Wawa has called in the FBI to probe data breach*, THE PHILADELPHIA INQUIRER, December 21, 2019 , available at https://www.inquirer.com/news/wawa-data-breach-credit-debit-card-fbi-investigation-20191221.html (last accessed Dec. 26, 2019).

20. It is well known in the retail industry that sensitive credit card information is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in payment systems either online or in stores."[3]

21. One commentator in the data security industry noted as to a previous, unrelated data breach:

> POS-malware breaches happen in the US with alarming regularity, and businesses should be well aware that they need to not only protect their central networks but also need to account for physical locations as well. . . . Moving forward, financial institutions should consider implementing a system of two-factor authentication in conjunction with a passive biometric solutions in order to mitigate the entirely avoidable outcomes of security incidents such as this.[4]

22. Despite the known risk of point-of-sale (POS) malware intrusions and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Wawa failed to take reasonable steps to adequately protect its computer systems and payment card environment from being breached, and then failed to detect the Data Breach for many months.

23. Wawa is, and at all relevant times has been, aware that the Card Information it maintains as a result of purchases made at its locations is highly sensitive and could be used for nefarious purposes by third parties.

24. Wawa's explicit statements in its Privacy Policy make clear that Wawa recognized

---

[3] Dennis Green and Mary Hanbury, *If you bought anything from these 11 companies in the last year, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 11:05 a.m.), available at https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed Dec. 16, 2019).

[4] *Cyber Attack on Earl Enterprises (Planet Hollywood)*, isBuzznews (Apr. 1, 2019), available at https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises-planet-hollywood/ (last accessed Dec. 16, 2019).

the importance of adequately safeguarding its customers' sensitive Card Information, yet Wawa failed to take the steps necessary to protect that sensitive data. On its website, Wawa's Privacy Policy provides the following:

> **Wawa Official Privacy Policy**
>
> Protecting your privacy is important to Wawa. This Wawa Privacy Policy ('Policy') describes how Wawa and its subsidiaries and affiliated companies collect, use, disclose and safeguard the personal information you provide on Wawa's websites, www.wawa.com and www.wawarewards.com, and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the "Sites") as well as information collected when you visit our stores or otherwise communicate or interact with Wawa.[5]

25. The Privacy Policy goes on to explain the types of information collected and how Wawa may use such information.

26. Wawa is thus aware of the importance of safeguarding its customers' Personal Information from the foreseeable consequences that would occur if its data security systems and computer servers were breached.

27. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

28. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Wawa to protect

[5] *See* Wawa Official Privacy Policy (Effective Date: May 2019), available at https://www.wawa.com/privacy (last accessed Dec. 20, 2019).

cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

29. The twelve requirements of the PCI DSS are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.[6]

30. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

31. Wawa was, at all material times, fully aware of its data protection obligations in light of its participation in the payment card processing networks and its daily collection and transmission of thousands of sets of Card Information.

32. Because Wawa accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that sensitive information

[6] PCI SECURITY STANDARDS COUNCIL, PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2, at 9 (May 2016), available at https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1506536983345 (last accessed Dec. 20, 2019).

secure from would-be data thieves in accordance with the PCI DSS requirements.

33. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

34. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

35. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[7]

36. The FTC has issued orders against businesses that failed to employ reasonable measures to secure payment card data. These orders provide further guidance to businesses with regard to their data security obligations.

37. As noted above, Wawa should have been and, based upon its acknowledged use of

[7] FEDERAL TRADE COMMISSION, Protecting Personal Information: A Guide for Business (Nov. 2011), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 20, 2019).

encryption technology at certain locations, was aware of the need to have adequate data security systems in place.

38. Despite this, Wawa failed to upgrade and maintain its data security systems in a meaningful way in order prevent data breaches. Wawa's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Wawa are in stark contrast and directly conflict with the PCI DSS core security standards.

39. Had Wawa properly maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach and/or could have promptly detected the Data Breach when it occurred.

40. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant and retail (and other) data breaches, Wawa was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

41. Wawa was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as, inter alia, Target, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty, Neiman Marcus, Michaels Stores, Hy-Vee, and Supervalu. As a result, Wawa was aware that malware is a real threat and is a primary tool of infiltration used by hackers seeking to carry out payment card breaches.

42. In addition to the publicly announced data breaches described above (among many others), Wawa knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of malware on July 31, 2014, and issued

a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[8]

43. Despite the fact that Wawa was on notice of the very real possibility of consumer data theft associated with its security practices and that Wawa knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted the Data Breach to continue for approximately nine months.

44. Wawa, at all times relevant to this action, had a duty to Plaintiff and members of the class to: (a) properly secure Personal Information submitted to or collected at Wawa's locations and on Wawa's internal networks; (b) encrypt Personal Information using industry standard methods; (c) use available technology to defend its systems from known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and class members, which would naturally result from Card Information theft; and (e) promptly notify customers when Wawa became aware that customers' Card Information may have been compromised.

45. Wawa permitted customers' Personal Information to be compromised by failing to take reasonable steps against a known threat.

46. In addition, leading up to the Data Breach, during the breach itself, and during the investigation that followed, Wawa failed to follow the guidelines set forth by the FTC.

47. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with

[8] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A (last accessed Dec. 20, 2019).

payment industry data security standards.[9]

48. The Data Breach is particularly egregious and Wawa's data security failures are particularly alarming given that the breach went undetected for so long, exposing millions of customers' sensitive data to criminals for nearly nine months. Clearly, had Wawa utilized adequate data security and data breach precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact significantly reduced (had the breach been permitted to occur at all).

49. With more than 850 Wawa locations potentially affected, and likely millions of individual's Personal Information stolen, this clearly marks a highly successful outing for criminals and a large failure on Wawa's part as to data security.

50. Because payment card data breaches involving malware are so common, and given the high level of data security measures available to companies that take customer payment information in, like Wawa, there is no reason why Wawa could not have adequately protected its systems and servers from the Data Breach.

51. As a result of the Data Breach, Plaintiff and class members suffered actual fraud and losses resulting from the Data Breach, including: financial losses related to the purchases made at Wawa that Plaintiff and class members would not have made had they known of Wawa's negligent approach to cybersecurity; lost control of consumers' Personal Information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; loss of time and money resolving fraudulent charges; loss of time and money

[9] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last accessed Dec. 20, 2019).

monitoring accounts for fraudulent transactions, loss of time and money obtaining protections against future identity theft; loss of rewards points or airline mileage available on credit cards that consumers lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information.

52. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

53. Furthermore, the Personal Information stolen from Wawa's locations can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

Data Breaches Lead to Identity Theft

54. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 26 million people were victims of one or more incidents of identity theft in 2016.[10]

55. Consumers' personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[11] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

56. According to the U.S. Department of Justice Bureau of Justice Statistics, an

[10] *See Victims of Identity Theft, 2016,* DOJ, at 1 (2019), available at https://www.bjs.gov/content/pub/pdf/vit16.pdf (last accessed Oct. 24, 2019).

[11] Companies, in fact, also recognize consumers' personal information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

estimated 26 million people were victims of one or more incidents of identity theft in 2016.[12]

The Monetary Value of Privacy Protections and Personal Information

57. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[13]

58. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[14]

59. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[15]

---

[12] *See Victims of Identity Theft, 2016*, DOJ, at 1 (2019), available at https://www.bjs.gov/content/pub/pdf/vit16.pdf (last accessed Nov. 15, 2019).

[13] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/publicevents/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last accessed November 11, 2019).

[14] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last accessed November 11, 2019).

[15] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. Recognizing the high value that consumers place on their personal information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their personal information.[16] This business has created a new market for the sale and purchase of this valuable data.[17]

62. Consumers place a high value not only on their personal information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2016 was $850." [18]

Damages Sustained by Plaintiff and the Other Class Members

63. Plaintiff and other members of the Class have suffered injury and damages,

---

accessed November 11, 2019).

[16] Steve Lohr, *You Want My Personal Data? Reward Me for It, The New York Times*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last accessed November 11, 2019).

[17] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last accessed November 11, 2019).

[18] See *Victims of Identity Theft, 2016*, DOJ, at 8 (2019), available at https://www.bjs.gov/content/pub/pdf/vit16.pdf (last accessed Nov. 15, 2019).

including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their personal and financial information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; and (iv) the value of their time and expenses associated with mitigation, remediation, and sorting out the risk of fraud and actual instances of fraud.

64. Plaintiff and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiff and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

COUNT I – NEGLIGENCE

65. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

66. Wawa owed to Plaintiff and the other Class members a duty to exercise reasonable care in handling and using the payment card data in its custody, including:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting payment card data in its possession;

b. to protect payment card data in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices and the practices and certifications represented on its website which it voluntarily undertook duties to implement; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly and sufficiently notifying Plaintiff and the other members of the Class of the Data Breach.

67. Wawa knew or should have known the risks of collecting and storing payment card data and the importance of maintaining secure systems.

68. Given the nature of Wawa's business, the sensitivity and value of the information

it maintains, and the resources at its disposal, Wawa should have identified the vulnerabilities for payment card purchases at Wawa's convenient stores and fuel pumps and prevented the Data Breach from occurring.

69. Defendant owed these duties to Plaintiff and the other Class members because Plaintiff and the other Class members are a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively profited from using Plaintiff and the other Class members' payment card information to process payments.

70. Wawa breached the duties it owed to Plaintiff and Class members in several ways, including:

a. by failing to implement adequate security systems, protocols and practices sufficient to protect payment card data and thereby creating a foreseeable, unreasonable risk of harm;

b. by failing to comply with the minimum industry data security standards and its own assurances of superior data security standards;

c. by negligently performing voluntary undertakings to secure and protect the payment card data it solicited and maintained; and

d. by failing to timely and sufficiently discover and disclose to consumers that their payment card data had been improperly acquired or accessed, and providing misleading and unfounded suggestions that their information (and by extension their identity) is not in the immediate peril it is in fact in.

e. But for Wawa's wrongful and negligent breach of the duties it owed to Plaintiff and the other Class members, their Personal Information would not have been compromised.

71. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Wawa's negligent conduct. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their payment card data, as well as

lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

72. Plaintiff's and the other Class members' injuries were proximately caused by Wawa's violations of the common law duties enumerated above, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT II – BREACH OF IMPLIED CONTRACT

73. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

74. In using credit or debit cards at Wawa stores, Plaintiff and the other members of the Class entered into an implied contract with Wawa, whereby Wawa became obligated to reasonably safeguard Plaintiff's and the other Class members' payment card data.

75. Under the implied contract, Wawa was obligated to not only safeguard payment card data, but also to provide Plaintiff and the other Class members with prompt, truthful, and adequate notice of any security breach or unauthorized access of said information.

76. Wawa breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard Plaintiff's payment card data.

77. Wawa also breached its implied contract with Plaintiff and the other Class members by failing to provide prompt, truthful, and adequate notice of the Data Breach and unauthorized access of their payment card data by hackers.

78. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) improper disclosure of their payment card data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon

them by the Data Breach; (iii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud; (iv) the increased risk of identity theft; and (v) deprivation of the value of their payment card data, which is likely to be sold to cyber criminals on the dark web.

COUNT III – UNJUST ENRICHMENT

79. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

80. Plaintiff and the other Class members conferred a monetary benefit on Wawa. Specifically, Plaintiffs and the other Class members paid for goods sold by Wawa and provided Wawa with payment information. In exchange, Plaintiffs and the other Class members were entitled to have Wawa protect their payment card data with adequate data security.

81. Wawa knew that Plaintiff and the other Class members conferred a benefit on Wawa. Wawa profited from Plaintiff's and the other Class members' purchases and used their payment card data for business purposes.

82. Wawa failed to secure Plaintiff's and the other Class members' payment card data and therefore did not provide full compensation for the benefit the Plaintiff and the other Class members provided. Wawa inequitably acquired the payment card data because it failed to disclose its inadequate security practices.

83. If Plaintiff and the other Class members knew that Wawa would not secure their payment card data using adequate security, they would not have shopped at Wawa's convenience stores and fuel pumps.

84. Plaintiff and the other Class members have no adequate remedy at law.

85. Under the circumstances, it would be unjust for Wawa to be permitted to retain any of the benefits that Plaintiff and the other Class members conferred on it.

86. Wawa should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and the other Class members proceeds that it unjustly received from them. In the alternative, Wawa should be compelled to refund the amounts that Plaintiff and the other Class members overpaid.

COUNT IV – NEGLIGENCE *PER SE*

87. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

88. Section 5 of the FTCA prohibits "unfair … practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wawa, of failing to use reasonable measures to protect payment card data.

89. Wawa violated Section 5 of the FTCA by failing to use reasonable measures to protect payment card data and not complying with applicable industry standards, as described herein. Wawa' conduct was particularly unreasonable given the nature and amount of payment card data it obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as Wawa, including, specifically, the damages that would result to Plaintiff and Class members.

90. Wawa' violation of Section 5 of the FTCA constitutes negligence *per se*.

91. Plaintiff and Class members are within the class of persons that the FTCA was intended to protect.

92. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

93. As a direct and proximate result of Wawa' negligence *per se*, Plaintiff and the Class will suffer injuries, including: inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach; false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and forgone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT V – DECLARATORY JUDGMENT

94. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

95. Plaintiff and members of the Class entered into an implied contract that required Defendant to provide adequate security for the personal information it collected from Plaintiff and Class members' payment card transactions.

96. Defendant owes duties of care to Plaintiff and the members of the Class which would require it to adequately secure personal information.

97. Defendant still possesses payment card data regarding Plaintiff and the Class members.

98. Because it has failed to discover the vulnerabilities in its security system which enabled the Data Breach to occur, Wawa still has not satisfied its contractual obligations and legal

duties to Plaintiffs. In fact, now that Wawa' lax approach towards information security, possibly as a result of cost-cutting, has become public, the personal information in Defendant's possession is more vulnerable than previously.

99. Actual harm has arisen in the wake of the Data Breach regarding its contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their personal information and Defendant's failure to address the security failings that lead to such exposure.

100. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited.

101. Plaintiff, therefore, seek a declaration that (1) Wawa' existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) to comply with its contractual obligations and duties of care, Wawa must implement and maintain reasonable security measures, including, but not limited to:

a. ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wawa' systems on a periodic basis, and ordering Wawa to promptly correct any problems or issues detected by such third-party security auditors;
b. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
c. ordering that Wawa audit, test, and train its security personnel regarding any new or modified procedures;
d. ordering that Wawa segment customer data by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;
e. ordering that Wawa purge, delete, and destroy in a reasonably secure manner

customer data not necessary for its provisions of services;

f. ordering that Wawa conduct regular database scanning and security checks;

g. ordering that Wawa routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Wawa to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Wawa customers must take to protect themselves.

CLASS ALLEGATIONS

102. Plaintiff brings this action on behalf of a Class, consisting of:

> All persons residing in the United States of America who made payment card purchases at affected locations during the affected time periods. Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

103. Plaintiff also brings this action on behalf of a Subclass, consisting of all members of the Class residing in the State of Pennsylvania.

104. The Class is so numerous that joinder is impracticable. Upon information and belief, there are tens or hundreds of thousands of members of the Class and tens of thousands of members of the Subclass.

105. There are questions of law and fact common to the members of the Class, which common questions predominate over any questions that affect only individual class members. The predominant common questions include:

a. Whether Wawa had a duty to protect Plaintiff and Class members' payment card data;

b. Whether Wawa knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Wawa's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Wawa was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Wawa's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Wawa's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the disclosure of Plaintiff and Class members' payment card data;

g. Whether Plaintiff and Class members are entitled to relief.

106. Plaintiff's claims are typical of the claims of the Class members. All are based on the same factual and legal theories.

107. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel experienced in consumer class action cases including data breach litigation.

108. A class action is superior to other alternative methods of adjudicating this dispute. Individual cases are not economically feasible.

JURY DEMAND

109. Plaintiff hereby demands a trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant for:

(a) actual damages;

(b) statutory damages;

(c) punitive damages;

(d) restitution;

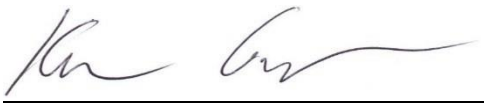
(e) injunctive relief;

(f) attorneys' fees, litigation expenses and costs of suit; and

(g) such other or further relief as the Court deems proper.

Dated: January 10, 2020

Respectfully submitted,



Kenneth J. Grunfeld
GOLOMB & HONIK, P.C.
1835 Market Street, Suite 2900
Philadelphia, PA 19103
(215) 278-4449
kgrunfeld@golombhonik.com

Shpetim Ademi
John D. Blythin
Mark A. Eldridge
Jesse Fruchter
ADEMI & O'REILLY, LLP
3620 East Layton Avenue
Cudahy, WI 53110
(414) 482-8000
(414) 482-8001 (fax)
sademi@ademilaw.com
jblythin@ademilaw.com
meldridge@ademilaw.com
jfruchter@ademilaw.com

JS 44 (Rev 02/19)

CIVIL COVER SHEET

20-cv-203

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

20 203

I. (a) PLAINTIFFS

Gary Nickerson, Individually and on Behalf of All Others Similarly Situated,

(b) County of Residence of First Listed Plaintiff Bucks
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Golomb & Honik, P.C.
1835 Market Street, Suite 2900
Philadelphia, PA 19103

DEFENDANTS

Wawa, Inc.

2020 JAN 10 P 1:37

USDC-EDPA
SEE FOR CLERK

County of Residence of First Listed Defendant Delaware
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for Nature of Suit Code Descriptions

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers Liability	PERSONAL PROPERTY		☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	LABOR	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 710 Fair Labor Standards Act	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 720 Labor/Management Relations	SOCIAL SECURITY	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 740 Railway Labor Act	☐ 861 HIA (1395ff)	☒ 480 Consumer Credit
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 751 Family and Medical Leave Act	☐ 862 Black Lung (923)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 790 Other Labor Litigation	☐ 863 DIWC/DIWW (405(g))	☐ 490 Cable/Sat TV
☐ 196 Franchise			☐ 791 Employee Retirement Income Security Act	☐ 864 SSID Title XVI	☐ 850 Securities/Commodities/ Exchange
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	☐ 865 RSI (405(g))	☐ 890 Other Statutory Actions
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:	☐ 462 Naturalization Application	FEDERAL TAX SUITS	☐ 891 Agricultural Acts
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 893 Environmental Matters
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 871 IRS - Third Party 26 USC 7609	☐ 895 Freedom of Information Act
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			☐ 896 Arbitration
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:			☐ 950 Constitutionality of State Statutes
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*
28 U.S.C. § 1332

Brief description of cause
Consumer Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000,000.00

CHECK YES only if demanded in complaint
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions)

JUDGE Gene E.K. Pratter DOCKET NUMBER 19-6019

DATE
01/10/2020

SIGNATURE OF ATTORNEY OF RECORD

JAN 10 2020

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

GEKP

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

20 203

DESIGNATION FORM
(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 1835 Market Street, Suite 2900, Philadelphia, PA 19103

Address of Defendant: Wawa, Inc., 260 W. Baltimore Pike, Wawa, Pennsylvania 19063

Place of Accident, Incident or Transaction: All Wawa Locations

RELATED CASE, IF ANY:

Case Number: 19-6019 Judge: Gene E.K. Pratter Date Terminated:

Civil cases are deemed related when *Yes* is answered to any of the following questions

		Yes	No
1	Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?	☐	☑
2	Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court?	☑	☐
3	Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court?	☐	☑
4	Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual?	☐	☑

I certify that, to my knowledge, the within case ☑ **is** / ☐ **is not** related to any case now pending or within one year previously terminated action in this court except as noted above

DATE: 01/10/2020 *Attorney-at-Law / Pro Se Plaintiff* 84121 *Attorney I.D. # (if applicable)*

CIVIL: (Place a √ in one category only)

A. Federal Question Cases

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
- ☐ 2 FELA
- ☐ 3 Jones Act-Personal Injury
- ☐ 4 Antitrust
- ☐ 5 Patent
- ☐ 6 Labor-Management Relations
- ☐ 7 Civil Rights
- ☐ 8 Habeas Corpus
- ☐ 9 Securities Act(s) Cases
- ☐ 10 Social Security Review Cases
- ☑ 11 All other Federal Question Cases
  (Please specify) CAFA

B. Diversity Jurisdiction Cases:

- ☐ 1 Insurance Contract and Other Contracts
- ☐ 2 Airplane Personal Injury
- ☐ 3 Assault, Defamation
- ☐ 4 Marine Personal Injury
- ☐ 5 Motor Vehicle Personal Injury
- ☐ 6 Other Personal Injury *(Please specify)*
- ☐ 7 Products Liability
- ☐ 8 Products Liability Asbestos
- ☐ 9 All other Diversity Cases
  (Please specify)

ARBITRATION CERTIFICATION
(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Kenneth J. Grunfeld, counsel of record *or* pro se plaintiff, do hereby certify

☑ Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs

☐ Relief other than monetary damages is sought

DATE: 01/20/2020 *Attorney-at-Law / Pro Se Plaintiff* 84121 *Attorney I.D. # (if applicable)*

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38

JAN 10 2020

Civ. 609 (5/2018)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CASE MANAGEMENT TRACK DESIGNATION FORM

GARY NICKERSON, Individually and on Behalf of All Others Similarly Situated, : CIVIL ACTION

v. : NO 20 203

Wawa, Inc.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

(a) Habeas Corpus – Cases brought under 28 U S.C. § 2241 through § 2255. ( )

(b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ( )

(c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53 2 ( )

(d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ( )

(e) Special Management - Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases) ( )

(f) Standard Management – Cases that do not fall into any one of the other tracks. (X)

01/10/2020	Kenneth J. Grunfeld	Plaintiff, Gary Nickerson
Date	**Attorney-at-law**	**Attorney for**
215-985-9177	215-985-4169	kgrunfeld@golombhonik.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02

JAN 10 2020